Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier

Rémi Blandino,[1,*] Anthony Leverrier,[2] Marco Barbieri,[1,†] Jean Etesse,[1] Philippe Grangier,[1] and Rosa Tualle-Brouri[1,3]

[1]*Laboratoire Charles Fabry, Institut d'Optique, Centre National de la Recherche Scientifique, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France*

[2]*Institute for Theoretical Physics, Eidgenössische Technische Hochschule Zurich, 8093 Zurich, Switzerland*

[3]*Institut Universitaire de France, 103 Boulevard St. Michel, 75005, Paris, France*

(Received 14 May 2012; published 23 July 2012)

We show that the maximum transmission distance of continuous-variable quantum key distribution in presence of a Gaussian noisy lossy channel can be arbitrarily increased using a heralded noiseless linear amplifier. We explicitly consider a protocol using amplitude- and phase-modulated coherent states with reverse reconciliation. Assuming that the secret key rate drops to zero for a line transmittance T_{lim}, we find that a noiseless amplifier with amplitude gain g can improve this value to T_{lim}/g^2, corresponding to an increase in distance proportional to $\log g$.

DOI: 10.1103/PhysRevA.86.012327 PACS number(s): 03.67.Dd

I. INTRODUCTION

Cryptography is certainly one of the most advanced applications of quantum technologies. Within this field, the most studied primitive is quantum key distribution (QKD), which is the art of distributing a secret key to two distant parties, Alice and Bob, in an untrusted environment controlled by an adversary, Eve [1]. The security of QKD rests on the idea that an adversary trying to acquire some information about the secret key will necessarily introduce some noise in the quantum communication between Alice and Bob. A consequence of this idea is that if the quantum channel is too lossy or noisy, then it cannot be used to distill a secret key. This limits the maximum transmission distance between the legitimate parties. Developing QKD protocols resistant to losses and noise is therefore of great practical importance.

Among QKD protocols, those encoding information in the amplitude and phase of coherent states [2,3] have the advantage of only requiring off-the-shelf telecom components, as well as being compatible with wavelength-division multiplexing [4], making an interesting solution for robust implementations [5,6].

On the theoretical side, these continuous-variable (CV) protocols have been proven secure against arbitrary attacks provided that they are secure against collective attacks [7]. This latter condition is in particular met for all CV protocols without postselection for which Gaussian attacks are known to be optimal within collective attacks [8–11].

Protocols with postselection on the other hand [12,13], where Alice and Bob only use part of their data to extract a secret key, can increase the robustness of QKD to losses and noise but at the price of more involved security proofs. In particular, their security is only established against Gaussian attacks [14,15], or when an active symmetrization of the classical data is applied [16].

In this paper, we consider the use of a heralded noiseless linear amplifier (NLA) [17–23] on the detection stage as a way to increase the robustness of CV QKD protocols against losses and noise. First, it should be noted that while amplifiers can effectively recover classical signals, they only offer limited advantages when working on quantum signals, as amplification is bound to preserve the original signal to noise ratio (SNR) [19,24,25]. This implies that ordinary linear amplifiers, as those realized by optical parametric processes [26], can only find limited applications in the context of QKD [27].

On the other hand, a *probabilistic* NLA can in principle amplify the amplitude of a coherent state while retaining the initial level of noise [17]. Thus, when only considering its successful runs, the NLA can compensate the effect of losses and could therefore be useful for quantum communication [28], and to establish the nonlocal nature of quantum correlations thanks to a loophole-free Bell test [29]. The availability of such a device has stimulated intense experimental activity over the past years, demonstrating the implementation of approximated versions [18–23], which have provided solid proof of principle.

The question arises if these more sophisticated devices can deliver a compensation of losses with a success rate such that it may represent a useful tool for quantum cryptography. Here we address this problem, by investigating the advantages and limitations of the most general NLA device, without making assumptions on the particular realization.

We find a regime in which the NLA leads to an improvement of the maximum transmission distance attainable on a noisy and lossy Gaussian channel. Because of the nondeterministic nature of the NLA, the security proofs considered here are similar to those concerning protocols with postselection, that is, they hold against Gaussian attacks, or collective attacks provided an additional symmetrization of the classical data is performed.

II. DESCRIPTION OF THE GROSSHANS AND GRANGIER PROTOCOL

We consider explicitly the case for the most common protocol for continuous-variable QKD, designed by Grosshans

[*] remi.blandino@institutoptique.fr

[†] Present address: Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU, United Kingdom.

and Grangier (GG02) [2], in its version with reverse reconciliation [3]. In a prepare-and-measure (PM) scheme, Alice encodes information in the quadratures of coherent states, which are then sent to Bob through the untrusted quantum channel. Alice chooses her preparation $|\alpha = x_{\mathrm{A}} + ip_{\mathrm{A}}\rangle$ from a Gaussian distribution for the two quadratures having zero mean and variance V_{A}. Bob randomly decides whether to measure the $\hat{x}$ or the $\hat{p}$ quadrature, using homodyne detection. Alice and Bob finally extract a secret key from the correlated data by performing classical data processing and authenticated classical communication. This protocol offers a simple experimental implementation [3,30–32] and is secure against finite-size collective attacks [33] as well as arbitrary attacks in the asymptotic limit of arbitrary long keys [7].

This protocol can be reformulated in an entanglement-based (EB) version, in terms of entanglement distribution between Alice and Bob [34]: the two parties initially share a two-mode squeezed vacuum state $|\lambda\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n\rangle|n\rangle$, with $\lambda < 1$. Alice performs a heterodyne measurement on her mode, which projects the other mode on a coherent state. The outcome of Alice's measurement is random, but with a probability distribution depending on λ.

Although the EB version does not correspond to the actual implementation, it is equivalent to the PM version from a security point of view, and it provides a more powerful description for establishing security proofs against collective attacks through the covariance matrix γ_{AB} of the state shared by Alice and Bob before their respective measurements. In the case of a Gaussian channel with transmittance T, and equivalent excess noise at the input ϵ [6]

$$\gamma_{\mathrm{AB}} = \begin{pmatrix} V(\lambda)\mathbb{I} & \sqrt{T[V(\lambda)^2-1]}\mathbb{Z} \\ \sqrt{T[V(\lambda)^2-1]}\mathbb{Z} & T[V(\lambda)+B+\epsilon]\mathbb{I} \end{pmatrix}, \qquad (1)$$

where $\mathbb{I} = \mathrm{diag}(1,1)$ and $\mathbb{Z} = \mathrm{diag}(1,-1)$, $V(\lambda) = \frac{1+\lambda^2}{1-\lambda^2}$ is the variance of the thermal state $\mathrm{Tr}_{\mathrm{A}}\,|\lambda\rangle\langle\lambda|$ related to the modulation variance by $V_{\mathrm{A}} = V - 1$, and $B = \frac{1-T}{T}$ is the equivalent input noise due to losses.

This matrix contains all the information needed to establish the secret key rate for collective attacks [30],

$$\Delta I(\lambda,T,\epsilon,\beta) = \beta I_{\mathrm{AB}}(\lambda,T,\epsilon) - \chi_{\mathrm{BE}}(\lambda,T,\epsilon), \qquad (2)$$

where $I_{\mathrm{AB}} = \frac{1}{2}\log_2(\frac{V+B+\epsilon}{1+B+\epsilon})$ is the mutual information shared by Alice and Bob given by Shannon's theory [35], and χ_{BE} is the Holevo bound for the mutual information shared by Eve and Bob (see Appendix B). The reconciliation efficiency $\beta<1$ accounts for the fact that in practical implementations of this protocol, Alice and Bob do not have sufficient resources to reach the Shannon limit. Steady progress has been made in recent years on the problem of error correction for CV QKD [36–38] and today's procedures based on modern error correcting techniques achieve $\beta \approx 95\%$ for a large range of SNR [39].

III. EQUIVALENT CHANNEL AND SQUEEZING

Let us now consider the use of a NLA in the GG02 protocol. As usual, we will perform the security analysis of the EB version. Here, we restrict ourselves to the case of a Gaussian quantum channel, that is Eve is limited to perform Gaussian attacks. Since the secure key rate of the protocol depends only on the covariance matrix of Alice and Bob γ_{AB}, it is sufficient to compute it in presence of the NLA.

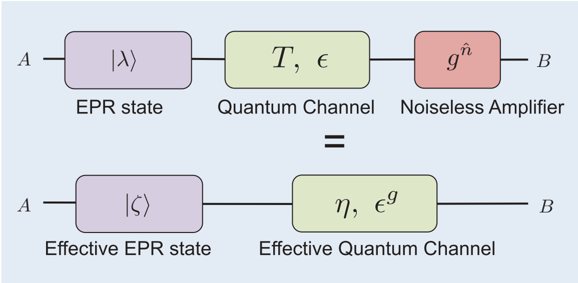

FIG. 1. (Color online) Equivalent channel and squeezing: a state $|\lambda\rangle$ sent through a Gaussian channel of transmittance T and excess noise ϵ, followed by a successful amplification, has the same Alice-Bob covariance matrix than a state $|\zeta\rangle$ sent through a Gaussian channel of transmittance η and excess noise ϵ^g, without the NLA.

In this modified version of the protocol, Alice and Bob implement GG02 as usual but Bob adds a NLA to his detection stage, before his homodyne detection, which is here assumed to be perfect. Then, only the events corresponding to a successful amplification will be used to extract a secret key. This scheme is therefore very similar to protocols with postselection.

Since the output of the NLA remains in the Gaussian regime, we can look for equivalent parameters of an EPR state sent through a Gaussian noisy channel. Their derivation is explained in detail in Appendix A, where it is shown that the covariance matrix $\gamma_{\mathrm{AB}}(\lambda,T,\epsilon,g)$ of the amplified state is equal to the covariance matrix $\gamma_{\mathrm{AB}}(\zeta,\eta,\epsilon^g,g=1)$ of an equivalent system with an EPR parameter ζ, sent through a channel of transmittance η and excess noise ϵ^g, without using the NLA (Fig. 1). Those effective parameters are given by

$$\begin{aligned}
\zeta &= \lambda\sqrt{\frac{(g^2-1)(\epsilon-2)T-2}{(g^2-1)\epsilon T-2}},\\
\eta &= \frac{g^2 T}{(g^2-1)T\left[\frac{1}{4}(g^2-1)(\epsilon-2)\epsilon T-\epsilon+1\right]+1},\\
\epsilon^g &= \epsilon - \frac{1}{2}(g^2-1)(\epsilon-2)\epsilon T.
\end{aligned} \qquad (3)$$

This identification easily provides the secret information ΔI^g corresponding to the successful amplification, since Eq. (2) can be used with the effective parameters

$$\Delta I^g(\lambda,T,\epsilon,\beta) = \Delta I(\zeta,\eta,\epsilon^g,\beta). \qquad (4)$$

Those parameters can be interpreted as physical parameters of an equivalent system if they satisfy the physical meaning constraints $0 \leqslant \zeta < 1$, $0 \leqslant \eta \leqslant 1$, and $\epsilon^g \geqslant 0$. Since λ is a global factor in the expression of ζ, the first condition is always satisfied if λ is below a limit value

$$0 \leqslant \zeta < 1 \Rightarrow 0 \leqslant \lambda < \left(\sqrt{\frac{(g^2-1)(\epsilon-2)T-2}{(g^2-1)\epsilon T-2}}\right)^{-1}. \qquad (5)$$

As η and ϵ^g do not depend on λ, the parameter ζ can be considered as independent of those two parameters, keeping in mind that this simply sets the value of λ.

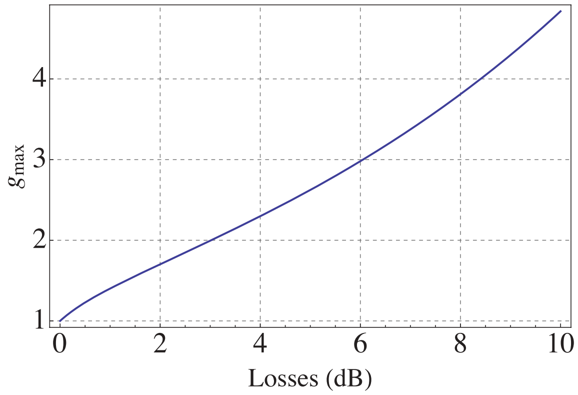

FIG. 2. (Color online) Maximum value of the gain $g_{\max}(T,\epsilon)$ as a function of the losses in dB, for $\epsilon = 0.2$.

The second and the third conditions are satisfied if the excess noise is smaller than 2, and if the gain is smaller than a maximum value given by Eq. (A19), and plotted on Fig. 2.

IV. INCREASE OF THE MAXIMUM TRANSMISSION DISTANCE

The analysis of the equivalent state allows us to compare the secret key rate obtained with and without an ideal NLA. The comparison must be performed for a given channel with fixed transmittance T and excess noise ϵ, as those parameters cannot be controlled by Alice or Bob. However, since the relevant quantity is the maximum secret key rate achievable over this channel, Alice is allowed to optimize her modulation variance V_{A} (or equivalently, the parameter λ) in order to maximize the secret key rate.

The secret key rate without the NLA is given by $\Delta I(\lambda,T,\epsilon,\beta)$ [Eq. (2)]. The secret key rate with the NLA ΔI_{NLA} is obtained by multiplying the secret key rate for successful amplifications ΔI^{g} by the probability of success P_{ss}. If the NLA has a sufficient dynamics to neglect distortions, we can assume that P_{ss} is constant. This is a reasonable assumption if $\beta < 1$, since in that case the optimal value of V_{A} is not infinite. The precise value of P_{ss} will depend on practical implementations, and is not important in our study, since it only acts as a scaling factor and does not change the fact that a negative secret key rate can become positive with a NLA. Therefore,

$$\Delta I_{\mathrm{NLA}} = P_{\mathrm{ss}} \Delta I(\zeta,\eta,\epsilon^{g}). \tag{6}$$

In Appendix D, we show that the probability of success for a NLA of gain g is upper bounded by $1/g^2$. We can therefore use this bound, keeping in mind that the relevant conclusion that can be taken is only whether the secret key rate is positive or not. Both secret key rates with and without the NLA are computed using the formulas given in Appendix B.

Since the expression of ΔI is relatively difficult to manipulate, we perform a series expansion at the first order in T, which corresponds to the strong losses regime (Appendix C). The approximate secret key rate is given by Eq. (C1). Its expression gives us an intuition about two important behaviors: first, since T appears inside the expansion and not only as a global factor, it explains why there can be a maximum transmission distance, or equivalently a value T_{lim} for which the secret key rate becomes null. Second, in this regime, the effect of the NLA is simply to replace T by g^2T, the other physical parameters being the same. Hence, it is clear that the losses are reduced, which will increase the maximum distance of transmission.

Let us prove those statements more precisely. From Eq. (C1), we find an analytical value of T_{lim} when $g = 1$ (i.e., without the NLA),

$$T_{\mathrm{lim}} = \frac{2}{\epsilon} \exp\left(\frac{\lambda^2(2\beta+\epsilon)-\epsilon}{\epsilon(\lambda^2-1)} - \frac{4\lambda^4}{\epsilon(\lambda^2-1)^2}\ln\lambda \right). \tag{7}$$

This expression clearly tends to 0 when ϵ tends to 0, which shows that there is no maximum transmission distance without excess noise. Interestingly, there is a maximum transmission distance as soon as the excess noise ϵ is nonzero, even if the reconciliation efficiency β equals 1. When β decreases or when ϵ increases, this maximum transmission distance decreases. There is no limitation of the distance of transmission only when $\epsilon = 0$, and in that case Eq. (C1) takes a simple form,

$$\Delta I_{\mathrm{NLA}} \simeq \frac{1}{g^2} g^2 T \lambda^2 \frac{(1-\lambda^2)(\beta - 2\ln\lambda) + 2\ln\lambda}{(\lambda^2-1)^2 \ln 2} \simeq \Delta I. \tag{8}$$

This shows that for strong losses without excess noise, the secret key rate using the NLA with the most optimistic probability of success is the same as the secret key rate without the NLA, and is always positive if λ is optimized. T_{lim} can also be optimized (i.e., minimized) by optimizing λ. Interestingly, the optimal value λ_{opt} depends only on β, as shown by Eq. (C2).

The same calculation with a NLA of gain g shows that

$$T_{\mathrm{lim}}^{g} = \frac{1}{g^2} T_{\mathrm{lim}}. \tag{9}$$

Therefore, the losses for which the secret key rate is zero are increased by

$$\Delta\mathfrak{L} = 20 \log_{10} g \text{ dB}. \tag{10}$$

Let us stress that this result does not depend on the probability of success of the NLA, which simply acts as a scaling factor for the secret key rate. Hence, even for a more realistic probability of success, the NLA increases the maximum transmission distance in the same way.

Those results are compared with numerical results for the full expressions of ΔI and ΔI_{NLA}, on Figs. 3 and 4. For both figures, the secret key rate is computed without the NLA and with a NLA of gain $g = 4$ (which is in the allowed region of Fig. 2).

Those figures clearly show that the secret key rate stays positive for losses increased by $\Delta\mathfrak{L} = 12$ dB. Figure 4 also shows that for given losses, the secret key rate stays positive for a higher value of excess noise. However, the increase in excess noise depends on the losses, and does not have a simple analytical expression.

Another important remark concerns the optimal gain. If the transmission can be intuitively improved by increasing the gain, this is not always the case for the secret key rate, as shown on Fig. 5. The first reason is the competition between the decreasing probability of success $1/g^2$ and the potential increase of the secret key rate for the successfully amplified states. The second reason is due to the dependence on the gain of the effective parameters [Eq. (3)]: the higher the gain, the higher η, but also the higher ϵ^{g}. If the gain is too high, it is

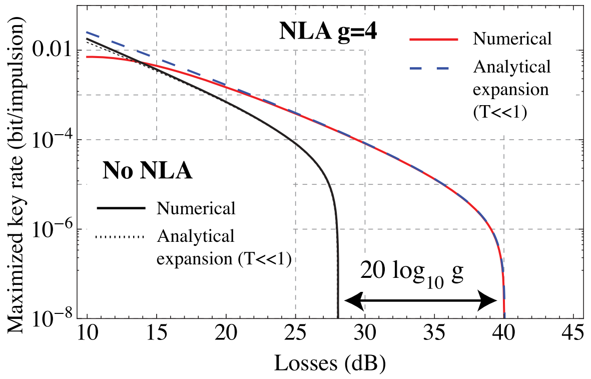

FIG. 3. (Color online) Maximized secret key rate as a function of the losses in dB. The maximization is performed on λ for the series expansion, and on ζ for the the numerical expression. The numerical curves are in excellent agreement with the series expansions. As explained in the main text, the secret key rate with the NLA is very optimistic due to the probability of success $1/g^2$, and hence its curve gives only information on its positivity. The other parameters are $\epsilon = 0.05$, $\beta = 0.95$ [39].

thus possible that the effective excess noise ϵ^g would be too important, for the transmittance η, to give a positive $\Delta I_{\rm NLA}$.

V. DISCUSSION AND CONCLUSION

In presence of excess noise, the secret key rate of the GG02 protocol against Gaussian collective attacks always becomes negative for a certain distance of transmission. We have shown that a heralded noiseless linear amplifier can increase this distance by the equivalent of $20 \log_{10} g$ dB of losses. We have also shown that for given losses, the protocol is more robust against excess noise.

Our calculation of the secret key rate with the amplifier was based on an effective system for which the security proofs are well established. This approach could also find applications in other quantum communication protocols involving an EPR state sent through a quantum channel, followed by a noiseless amplifier. In particular, it could be applied to other CV QKD protocols, for instance protocols using squeezed states, or protocols using an heterodyne detection [40–43].

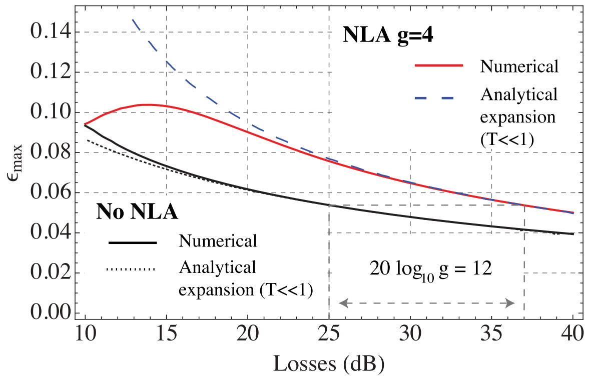

FIG. 4. (Color online) Maximal excess noise for which the secret key rate is positive, as a function of the losses in dB. The curves do not depend on the probability of success chosen for the NLA. The maximization is performed on λ for the series expansion, and on ζ for the numerical expression. For low losses, we see that the first-order expansion is not enough, whereas it is in excellent agreement with the numerical curve for strong losses. The reconciliation efficiency is $\beta = 0.95$ [39].

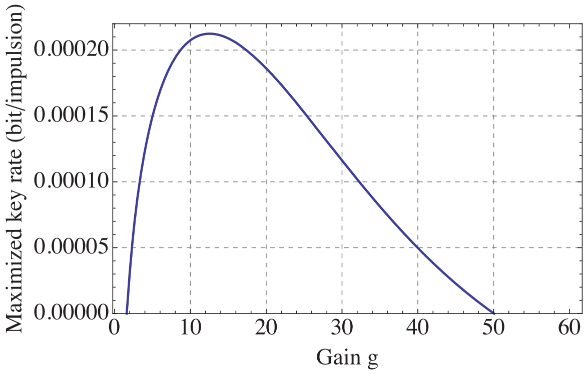

FIG. 5. (Color online) Maximized secret key rate as a function of the gain of the NLA, with a probability of success $1/g^2$, and parameters $\beta = 1$, $\epsilon = 0.1$, 30 dB of losses. With a gain $g = 1$, the secret key rate is negative. The NLA can increase the secret key rate to positive values when the gain is increased, however if the gain is too large the secret key rate decreases and becomes negative again. The reason is that the effective excess noise becomes too large to be acceptable given the effective transmittance.

Further work would be to consider the experimentally demonstrated schemes of the NLA, which are only valid approximations of the ideal NLA up to a certain number of photons. If the state can be well approximated by this truncation, so that the Gaussian approximation still holds, the results presented in this paper are still valid. On the other hand, if the Gaussian approximation does not hold anymore, security proofs are more complicated to manipulate. This problem lies beyond the scope of the present work, and deserves further investigation.

Finally, two recent preprints [44,45] reach similar conclusions, and also show that it might be possible to operate a "virtual" noiseless amplifier by performing postprocessing on the data.

ACKNOWLEDGMENTS

We acknowledge support from the EU project ANR ERA-Net CHISTERA HIPERCOM. M.B. is supported by the Marie Curie contract PIEF-GA-2009-236345-PROMETEO. A.L. was supported by the SNF through the National Centre of Competence in Research "Quantum Science and Technology".

APPENDIX A: DERIVATION OF THE EFFECTIVE PARAMETERS

In this Appendix, we detail the method used to obtain the effective parameters of Sec. III. Let us start by first computing the output of the NLA when the input state $\hat{\rho}$ is a thermal state $\hat{\rho}_{\rm th}(\lambda_{\rm ch}) = (1-\lambda_{\rm ch}^2)\sum_{n=0}^{\infty}\lambda_{\rm ch}^{2n}|n\rangle\langle n|$ displaced by $\beta = \beta_{\rm x} + i\beta_{\rm y}$

$$\hat{\rho} = \hat{D}(\beta)\hat{\rho}_{\rm th}(\lambda_{\rm ch})\hat{D}(-\beta). \tag{A1}$$

This would be the state received by Bob if he knew the result of Alice's heterodyne measurement. The state $\hat{\rho}$ can be decomposed on an ensemble of coherent states using the P function [46],

$$\hat{\boldsymbol{\rho}} = \int P(\alpha)|\alpha\rangle\langle\alpha|\mathrm{d}\alpha, \tag{A2}$$

where $P(\alpha) = \frac{e^{|\alpha|^2}}{\pi^2}\int e^{|u|^2}\langle -u|\hat{\boldsymbol{\rho}}|u\rangle e^{u^*\alpha - u\alpha^*}\mathrm{d}u$. Straightforward calculations show that $\langle -u-\beta|\hat{\boldsymbol{\rho}}_{\mathrm{th}}(\lambda_{\mathrm{ch}})|u-\beta\rangle = (1-\lambda_{\mathrm{ch}}^2)e^{-|u|^2(1+\lambda_{\mathrm{ch}}^2)-|\beta|^2(1-\lambda_{\mathrm{ch}}^2)+(u\beta^*-u^*\beta)(1-\lambda_{\mathrm{ch}}^2)}$, and therefore $P(\alpha_{\mathrm{x}}+i\alpha_{\mathrm{y}}) = p(\alpha_{\mathrm{x}})p(\alpha_{\mathrm{y}})$, with

$$p(\alpha_{\mathrm{x}}) = \frac{1}{\sqrt{\pi}}\sqrt{\frac{1-\lambda_{\mathrm{ch}}^2}{\lambda_{\mathrm{ch}}^2}e^{-\frac{1-\lambda_{\mathrm{ch}}^2}{\lambda_{\mathrm{ch}}^2}(\alpha_{\mathrm{x}}-\beta_{\mathrm{x}})^2}}. \tag{A3}$$

In the absence of thermal noise ($\lambda_{\mathrm{ch}} = 0$), the expression (A3) becomes proportional to a Dirac distribution $\delta(\alpha_{\mathrm{x}} - \beta_{\mathrm{x}})$. The same statements hold for $p(\alpha_{\mathrm{y}})$.

The successful amplification can ideally be described by an operator $\hat{\boldsymbol{C}} = g^{\hat{n}}$, where $\hat{n}$ is the number operator in the Fock basis. The final state has to be normalized, but one has to be careful that the norm is not the success probability of the transformation, since $\hat{\boldsymbol{C}}$ is unbounded. The amplification of a coherent state $|\alpha\rangle$ leads to an amplified coherent state proportional to $|g\alpha\rangle$

$$\hat{\boldsymbol{C}}|\alpha\rangle = e^{\frac{|\alpha|^2}{2}(g^2-1)}|g\alpha\rangle. \tag{A4}$$

Since $\hat{\boldsymbol{C}}$ is linear, the amplification of $\hat{\boldsymbol{\rho}}$ is simple to derive, using (A3) and (A4) in the decomposition (A2),

$$\hat{\boldsymbol{\rho}}' = \hat{\boldsymbol{C}}\hat{\boldsymbol{\rho}}\hat{\boldsymbol{C}} \tag{A5}$$

$$= \int P(\alpha)e^{|\alpha|^2(g^2-1)}|g\alpha\rangle\langle g\alpha|\mathrm{d}\alpha. \tag{A6}$$

By introducing the change of variable $u = g\alpha$, one gets

$$\hat{\boldsymbol{\rho}}' \propto \int P(u/g)e^{\frac{g^2-1}{g^2}|u|^2}|u\rangle\langle u|\mathrm{d}u. \tag{A7}$$

As before, it is easy to see that $P(u/g) = p(u_{\mathrm{x}}/g)p(u_{\mathrm{y}}/g)$. Since $|u|^2 = u_{\mathrm{x}}^2+u_{\mathrm{y}}^2$, we can only consider the term $p(u_{\mathrm{x}}/g)\exp(\frac{g^2-1}{g^2}u_{\mathrm{x}}^2)$, the results being similar for u_{y}

$$p(u_{\mathrm{x}}/g)e^{\frac{g^2-1}{g^2}u_{\mathrm{x}}^2} = \frac{1}{\sqrt{\pi}}\sqrt{\frac{1-\lambda_{\mathrm{ch}}^2}{\lambda_{\mathrm{ch}}^2}e^{-\frac{1-\lambda_{\mathrm{ch}}^2}{\lambda_{\mathrm{ch}}^2}(\frac{u_{\mathrm{x}}}{g}-\beta_{\mathrm{x}})^2+\frac{g^2-1}{g^2}u_{\mathrm{x}}^2}}. \tag{A8}$$

The argument of the exponential can be easily put in the form

$$\begin{aligned} -\frac{1-\lambda_{\mathrm{ch}}^2}{\lambda_{\mathrm{ch}}^2}\left(\frac{u_{\mathrm{x}}}{g}-\beta_{\mathrm{x}}\right)^2 + \frac{g^2-1}{g^2}u_{\mathrm{x}}^2 \\ = \underbrace{-\frac{1-g^2\lambda_{\mathrm{ch}}^2}{g^2\lambda_{\mathrm{ch}}^2}}_{\text{Thermal state } g\lambda_{\mathrm{ch}}}\left(u_{\mathrm{x}} - \beta_{\mathrm{x}}\underbrace{g\frac{1-\lambda_{\mathrm{ch}}^2}{1-g^2\lambda_{\mathrm{ch}}^2}}_{\text{Effective gain}}\right)^2 \\ \underbrace{-\beta_{\mathrm{x}}^2\frac{(1-g^2)(1-\lambda_{\mathrm{ch}}^2)}{1-g^2\lambda_{\mathrm{ch}}^2}}_{\text{Normalization term}}. \end{aligned} \tag{A9}$$

Thus, the expression (A9) clearly corresponds to a thermal state $\hat{\boldsymbol{\rho}}_{\mathrm{th}}(g\lambda_{\mathrm{ch}})$ displaced by $g\frac{1-\lambda_{\mathrm{ch}}^2}{1-g^2\lambda_{\mathrm{ch}}^2}\beta$, up to a global unimportant normalization factor independent of the variable integrated α or u. We can conclude that

$$\hat{\boldsymbol{\rho}}' \propto \hat{\boldsymbol{D}}(\tilde{g}\beta)\hat{\boldsymbol{\rho}}_{\mathrm{th}}(g\lambda_{\mathrm{ch}})\hat{\boldsymbol{D}}(-\tilde{g}\beta), \tag{A10}$$

where $\tilde{g} = g\frac{1-\lambda_{\mathrm{ch}}^2}{1-g^2\lambda_{\mathrm{ch}}^2}$. In order to keep a physical interpretation, we note that g must be such that $g\lambda_{\mathrm{ch}}<1$.

Let us now find the values of β and λ_{ch} corresponding to the entanglement-based protocol presented in the main text. When Alice obtains the results α_{A} for her heterodyne measurement on one mode of the EPR state $|\lambda\rangle$, the second mode is projected on a coherent state with an amplitude proportional to $\lambda\alpha_{\mathrm{A}}$ [34]. This state is then sent through the quantum channel of transmittance T, which transforms its amplitude to $\propto \sqrt{T}\lambda\alpha_{\mathrm{A}}$. The displacement β can thus be taken as

$$\beta = \sqrt{T}\lambda\alpha_{\mathrm{A}}. \tag{A11}$$

The variance $\frac{1+\lambda_{\mathrm{ch}}^2}{1-\lambda_{\mathrm{ch}}^2}$ of the thermal state corresponds to Bob's variance $1+T\epsilon$ when $V_{\mathrm{A}} = 0$,

$$\frac{1+\lambda_{\mathrm{ch}}^2}{1-\lambda_{\mathrm{ch}}^2} = 1 + T\epsilon \Rightarrow \lambda_{\mathrm{ch}}^2 = \frac{T\epsilon}{2+T\epsilon}. \tag{A12}$$

Finally, the action of the NLA [Eq. (A10)] on a displaced thermal state given by Eqs. (A11) and (A12) induces the transformations

$$\begin{aligned} \sqrt{T}\lambda\alpha_{\mathrm{A}} &\underset{\mathrm{NLA}}{\rightarrow} g\frac{1-\lambda_{\mathrm{ch}}^2}{1-g^2\lambda_{\mathrm{ch}}^2}\sqrt{T}\lambda\alpha_{\mathrm{A}}, \\ \frac{T\epsilon}{2+T\epsilon} &\underset{\mathrm{NLA}}{\rightarrow} g^2\frac{T\epsilon}{2+T\epsilon}. \end{aligned} \tag{A13}$$

The next step is to consider the action of the NLA when Bob does not have any knowledge on Alice's measurement outcome. In such a case, his state is a thermal state $\hat{\boldsymbol{\rho}}_{\mathrm{B}} = (1-\lambda^{\star 2})\sum_{n=0}^{\infty}(\lambda^{\star})^{2n}|n\rangle\langle n|$, whose variance is given by γ_{AB}

$$\begin{aligned} \frac{1+\lambda^{\star 2}}{1-\lambda^{\star 2}} &= 1 + TV_{\mathrm{A}} + T\epsilon \Rightarrow \\ \lambda^{\star 2} &= \frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2-\lambda^2[2+T(\epsilon-2)]+T\epsilon}. \end{aligned} \tag{A14}$$

Since the NLA always transforms a thermal state of parameter $\lambda^{\star}$ into another thermal state of parameter $g\lambda^{\star}$, Eq. (A14) shows that the NLA performs the transformation

$$\begin{aligned} &\frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2-\lambda^2[2+T(\epsilon-2)]+T\epsilon} \\ &\underset{\mathrm{NLA}}{\rightarrow} g^2\frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2-\lambda^2[2+T(\epsilon-2)]+T\epsilon}. \end{aligned} \tag{A15}$$

We have now all the required equations to find the expression of the effective parameters ζ, η, and ϵ^g. Using Eqs. (A13) and (A15), those parameters must satisfy

$$\begin{aligned} \sqrt{\eta}\zeta &= g\frac{1-\lambda_{\mathrm{ch}}^2}{1-g^2\lambda_{\mathrm{ch}}^2}\sqrt{T}\lambda, \\ \frac{\eta\epsilon^g}{2+\eta\epsilon^g} &= g^2\frac{T\epsilon}{2+T\epsilon}, \\ \frac{\eta[\zeta^2(2-\epsilon^g)+\epsilon^g]}{2-\zeta^2[2+\eta(\epsilon^g-2)]+\eta\epsilon^g} &= g^2\frac{T[\lambda^2(2-\epsilon)+\epsilon]}{2-\lambda^2[2+T(\epsilon-2)]+T\epsilon}. \end{aligned} \tag{A16}$$

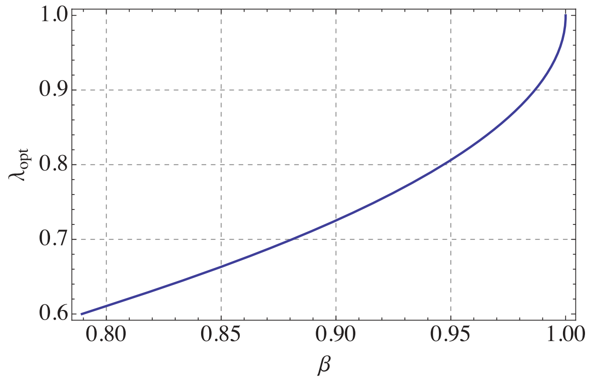

FIG. 6. (Color online) Optimized two-mode squeezing parameter λ_{opt} as a function of β. The value $\beta = 0.95$ gives $\lambda_{\text{opt}} \simeq 0.806$.

This system can be solved, leading to

$$\zeta = \lambda\sqrt{\frac{(g^2-1)(\epsilon-2)T-2}{(g^2-1)\epsilon T-2}},$$

$$\eta = \frac{g^2T}{(g^2-1)T\left[\frac{1}{4}(g^2-1)(\epsilon-2)\epsilon T-\epsilon+1\right]+1},$$

$$\epsilon^g = \epsilon + \frac{1}{2}(g^2-1)(2-\epsilon)\epsilon T. \tag{A17}$$

Finally, the expression of the maximum gain $g_{\max}(T,\epsilon)$ for which those parameters take physical values is given by

$$g_{\max}(T,\epsilon) = \sqrt{\frac{\epsilon[T(\epsilon-4)+2]+4\sqrt{\frac{T(\epsilon-2)+2}{\epsilon}}-2\sqrt{\epsilon[T(\epsilon-2)+2]}+4T-4}{T(\epsilon-2)^2}}. \tag{A18}$$

Let us stress some important comments about those effective parameters, which confirm the validity of their expression. First, they naturally reduce to the real physical parameters without the NLA, for $g = 1$,

$$g = 1 \Rightarrow \begin{cases} \zeta = \lambda \\ \eta = T \\ \epsilon^g = \epsilon \end{cases}. \tag{A19}$$

Then, when there is no excess noise ($\epsilon = 0$), they match previous results [17],

$$\epsilon = 0 \Rightarrow \begin{cases} \zeta = \lambda\sqrt{1+(g^2-1)T} \\ \eta = \frac{g^2T}{1+(g^2-1)T} \\ \epsilon^g = 0 \end{cases}. \tag{A20}$$

APPENDIX B: EXPRESSIONS USED TO COMPUTE THE HOLEVO BOUND χ_{BE}

The Holevo bound χ_{BE} is given by [30]: $\chi_{\text{BE}} = G(\frac{\mu_1-1}{2}) + G(\frac{\mu_2-1}{2}) - G(\frac{\mu_3-1}{2}) - G(\frac{\mu_4-1}{2})$ where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x$$
$$\text{if } \; x \neq 0, \quad \text{and } \; G(0) = 0 \tag{B1}$$

$$\mu_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2-4E}) \quad \mu_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2-4D}) \tag{B2}$$

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{\text{line}})^2$$
$$E = T^2(V\chi_{\text{line}}+1)^2 \tag{B3}$$

$$C = \frac{V\sqrt{E}+T(V+\chi_{\text{line}})}{T(V+\chi_{\text{line}})} \qquad D = \frac{\sqrt{E}V}{T(V+\chi_{\text{line}})} \tag{B4}$$

$V = V_{\text{A}} + 1$ is the variance of Alice's thermal state (see text for details), and $\chi_{\text{line}} = \frac{1-T}{T} + \epsilon$ is the total equivalent input noise. Bob's homodyne detection is assumed to be perfect.

APPENDIX C: FIRST-ORDER EXPANSION IN *T*

The first order expansion in T of the secret key rate given in Appendix B using the NLA is:

$$\Delta I_{\text{NLA}} \simeq P_{\text{ss}} g^2 T \frac{-2\beta\lambda^2(-1+\lambda^2) - \epsilon(-1+\lambda^2)^2(1+\ln 2)+(-1+\lambda^2)[\epsilon(-1+\lambda^2)(\ln\epsilon+\ln g^2T)+4\lambda^2\ln\lambda]+2\lambda^2\ln\lambda^2}{2(-1+\lambda^2)^2\ln 2}. \tag{C1}$$

The equation that must satisfy the optimal value λ_{opt} to maximize the transmission distance (Eq. (7)), and maximize the secret key rate (Eq. (C1)), is given by:

$$\frac{\lambda_{\text{opt}}^2(\lambda_{\text{opt}}^2 - 4\ln\lambda_{\text{opt}} - 1)}{1-\lambda_{\text{opt}}^2} = \beta. \tag{C2}$$

Figure 6 shows λ_{opt} as a function of β.

APPENDIX D: SUCCESS PROBABILITY

The success probability of the NLA can depend on many experimental factors. Here, we are interested in deriving an upper bound based on very general principles, when the success probability can be considered as being a constant value. In this way, we can obtain an optimistic estimate of its performance, but certainly we will not overlook interesting regimes. In both EB and PM versions of the GG02 protocol, Bob's state prior to any classical communication with Alice is the thermal state $\hat{\rho}_{\text{B}}(\lambda^\star) = (1-\lambda^{\star 2})\sum_{n=0}^{\infty}(\lambda^\star)^{2n}|n\rangle\langle n|$.

Consider now that the NLA produces an amplified state $\hat{\rho}_{\mathrm{B}}(g\lambda^\star)$ with a success probability P_{ss}. When the amplification fails, the protocol is aborted and the state is simply replaced by the vacuum $|0\rangle\langle 0|$. Without postselection, the NLA can therefore be represented as a trace-preserving operation $\mathcal{T}$ described by

$$\mathcal{T}[\hat{\rho}_{\mathrm{B}}(\lambda^\star)] = P_{\mathrm{ss}}\hat{\rho}_{\mathrm{B}}(g\lambda^\star) + (1 - P_{\mathrm{ss}})|0\rangle\langle 0|. \quad \text{(D1)}$$

Naturally, $\mathcal{T}$ applied on the vacuum also gives the vacuum, regardless of the value of P_{ss}. Since any trace-preserving quantum operation cannot decrease the fidelity $\mathcal{F}$ between two quantum states [47], $\mathcal{T}$ must verify

$$\mathcal{F}(\hat{\rho}_{\mathrm{B}}(\lambda^\star), |0\rangle\langle 0|) \leqslant \mathcal{F}(\mathcal{T}[\hat{\rho}_{\mathrm{B}}(g\lambda^\star)], |0\rangle\langle 0|), \quad \text{(D2)}$$

which gives us an upper bound on P_{ss}. Indeed, inserting the expression for Bob's transformed state [Eq. (D1)] in the constraints on fidelities [Eq. (D2)], we find that P_{ss} must verify

$$\langle 0|\hat{\rho}_{\mathrm{B}}(\lambda^\star)|0\rangle \leqslant \langle 0|(P_{\mathrm{ss}}\hat{\rho}_{\mathrm{B}}(g\lambda^\star) + (1 - P_{\mathrm{ss}})|0\rangle\langle 0|)|0\rangle, \quad \text{(D3)}$$

which is satisfied if

$$P_{\mathrm{ss}} \leqslant \frac{1}{g^2}. \quad \text{(D4)}$$

[1] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[4] B. Qi, W. Zhu, L. Qian, and H. Lo, New J. Phys. **12**, 103042 (2010).

[5] N. J. Cerf and P. Grangier, J. Opt. Soc. Am. B **24**, 324 (2007).

[6] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[7] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[8] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[9] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[10] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).

[11] A. Leverrier and P. Grangier, Phys. Rev. A **81**, 062314 (2010).

[12] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[13] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[14] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[15] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[16] A. Leverrier, Phys. Rev. A **85**, 022339 (2012).

[17] T. C. Ralph and A. P. Lund, in Quantum Communication Measurement and Computing Proceedings of 9th International Conference, edited by A. Lvovsky, AIP Conf. Proc. No. 1110 (AIP, New York, 2009), pp. 155–160, arXiv:0809.0326.

[18] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[19] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **83**, 063801 (2011).

[20] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, Laser Phys. Lett. **8**, 411 (2011).

[21] A. Zavatta, J. Fiurasek, and M. Bellini, Nature Photon. **5**, 52 (2011).

[22] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nature Photon. **4**, 316 (2010).

[23] M. A. Usuga, C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nature Phys. **6**, 767 (2010).

[24] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[25] J. A. Levenson, I. Abram, T. Rivera, and P. Grangier, J. Opt. Soc. Am. B **10**, 2233 (1993).

[26] R. Loudon, The Quantum Theory of Light (Oxford University Press, Oxford, 2000).

[27] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).

[28] T. C. Ralph, Phys. Rev. A **84**, 022339 (2011).

[29] J. B. Brask, N. Brunner, D. Cavalcanti, and A. Leverrier, Phys. Rev. A **85**, 042116 (2012).

[30] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[31] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[32] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache *et al.*, Optics Express **20**,14030 (2012).

[33] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[34] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[35] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).

[36] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. M. Merolla, in *IEEE Information Theory Workshop, 2006, ITW '06 Punta del Este* (IEEE, Uruguay, 2006), pp. 116–120.

[37] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).

[38] P. Jouguet and S. Kunz-Jacques, arXiv:1204.5882.

[39] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[40] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[41] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[42] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. A **73**, 022316 (2006).

[43] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[44] J. Fiurasek and N. J. Cerf, arXiv:1205.6933.

[45] N. Walk, T. Symul, P. K. Lam, and T. C. Ralph, arXiv:1206.0936.

[46] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, 2005).

[47] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).